# Safety and Fitness Electronic Records System (SAFER)

# User and System Requirements Document

Updated October, 1996

October 28, 1996

PL-96-0603

Prepared for:


Federal Highway Administration

Prepared by:


The Johns Hopkins University
Applied Physics Laboratory

## Table of Contents


| | | |
|---|---|---|
| 1.0 | Introduction | 1 |
| 1.1 | Purpose | 1 |
| 1.2 | Scope | 1 |
| 2.0 | General Description | 2 |
| 2.1 | System Perspective | 2 |
| 2.2 | System Functions | 2 |
| 3.0 | Functional Requirements | 2 |
| 3.1 | User Services | 3 |
| 3.1.1 | Search/Verify a Carrier | 3 |
| 3.1.1.1 | Search Input | 4 |
| 3.1.1.1.1 | Pre-Formatted Queries | 4 |
| 3.1.1.1.2 | Cost Check | 4 |
| 3.1.1.2 | Search Processing | 4 |
| 3.1.1.2.1 | Fuzzy Searching | 4 |
| 3.1.1.3 | Search Output | 4 |
| 3.1.1.3.1 | Maximum Carriers Returned | 4 |
| 3.1.1.3.2 | Multiple Match Format | 5 |
| 3.1.2 | Provide Carrier Snapshot Report | 5 |
| 3.1.2.1 | Snapshot Input Definition | 5 |
| 3.1.2.1.1 | User Input For Snapshots | 5 |
| 3.1.2.1.2 | Snapshot Data Sources | 5 |
| 3.1.2.1.3 | Auth. Source Updates-Snapshots | 5 |
| 3.1.2.1.4 | Snapshot Update Format | 6 |
| 3.1.2.2 | Snapshot Processing Definition | 6 |
| 3.1.2.2.1 | Snapshot Data Extraction | 6 |
| 3.1.2.2.2 | Snapshot Routing | 6 |
| 3.1.2.2.3 | Snapshot Refresh | 6 |
| 3.1.2.3 | Snapshot Output Definition | 6 |
| 3.1.2.3.1 | Standard Snapshot Output | 6 |
| 3.1.2.3.2 | Snapshot Views | 6 |
| 3.1.3 | Detailed Carrier Profile Report | 7 |
| 3.1.3.1 | Profile Input Definition | 7 |
| 3.1.3.1.1 | User Input For Profiles | 7 |
| 3.1.3.1.2 | Auth. Source Input For Profiles | 7 |
| 3.1.3.2 | Profile Processing Definition | 7 |
| 3.1.3.2.1 | Profile Data Extraction | 8 |
| 3.1.3.2.2 | Profile Routing | 8 |
| 3.1.3.2.3 | Duplicate Profile Requests | 8 |
| 3.1.3.2.4 | Pending Profile Data | 8 |
| 3.1.3.4 | Profile Outputs Definition | 8 |
| 3.1.3.4.1 | Standard Profile Output | 8 |
| 3.1.3.4.2 | Profile Cache | 8 |
| 3.1.4 | Carrier "Subscriber" Capability | 9 |

## Table of Contents


| | | |
|---|---|---|
| 3.1.4.1 | Subscriber List Input | 9 |
| **3.1.4.2** | Subscriber List Processing | 9 |
| 3.1.4.2.1 | Subscriber List Trigger Process | 10 |
| 3.1.4.2.2 | Threshold/Event Translation | 10 |
| 3.1.4.2.3 | Update Event Table | 10 |
| 3.1.4.2.4 | Automated Subscriber Update | 10 |
| 3.1.4.2.5 | Types of Events Monitored | 10 |
| 3.1.4.2.6 | Determination of Event | 10 |
| 3.1.4.2.7 | Subscriber Response Time | 10 |
| 3.1.4.3 | Subscriber List Output Def. | 11 |
| 3.1.4.3.1 | Subscriber List Output | 11 |
| 3.1.4.3.2 | Event Monitoring Report | 11 |
| 3.1.4.3.3 | Subscriber Status Report | 11 |
| 3.1.4.4 | Subscriber User Update | 11 |
| 3.1.5 | Aggregate Data Requests | 11 |
| 3.1.5.1 | Aggregate Data Request Input | 11 |
| 3.1.5.2 | Aggregate Data Req. Processing | 12 |
| 3.1.5.3 | Aggregate Data Request Output | 12 |
| 3.2 | Establish/Maintain User Account | 12 |
| 3.2.1 | User Account Input | 12 |
| 3.2.1.1 | Organizational Account | 12 |
| 3.2.2 | User Account Processing | **12** |
| 3.2.2.1 | User Account Update Processing | 12 |
| 3.2.2.2 | User Account Access Privilege | 13 |
| 3.2.2.3 | Request Cancellation | 13 |
| 3.2.2.4 | User Requests Waiting | 13 |
| 3.2.3 | User Account Output | 13 |
| 3.2.3.1 | User Account Status Fields | 13 |
| 3.2.3.2 | User Documentation | 13 |
| 3.2.3.3 | User Software | 13 |
| 3.3 | Monitor System Activity/Billing | 13 |
| 3.3.1 | System Activity Logging | 14 |
| 3.3.2 | Privacy Access Transaction Log | 14 |
| 3.3.3 | Network Billing | 14 |
| 3.4 | External System Data Access | 14 |
| 3.4.1 | Accessing Authoritative Sources | 14 |
| 3.4.1.1 | Authoritative Source Ack. | 15 |
| 3.4.1.2 | Authoritative Src. Data Receipt | 15 |
| 3.4.2 | Access Roadside Inspection Site | 15 |
| 3.4.3 | Inter-User Data Flow Definition | 15 |
| 3.4.3.1 | Inter-User Data Exchange | 15 |
| 3.4.3.2 | Inter-User Data Routing | 15 |
| 3.4.4 | Base State Routing | 15 |

## Table of Contents


| | | |
|---|---|---|
| 3.5 | Vehicle/Driver Data Support | 16 |
| 3.5.1 | Inspection Report Support | 16 |
| 3.5.1.1 | Inspection Reports:Phase 1 | 16 |
| 3.5.1.1.1 | Inspection Rpts:P-1 Receipt | 16 |
| 3.5.1.1.2 | Inspection Rpts:P- 1 Storage | 16 |
| 3.5.1.1.3 | Inspection Rpts:P-1 Deletion | 16 |
| 3.5.1.1.4 | Insp. Rpts:P-1 Mailbox Access | 17 |
| 3.5.1.2 | Inspection Reports:Phase 2 | 17 |
| 3.5.1.2.1 | Insp. Rpts:P-2 Mailbox Access | 17 |
| 3.5.1.2.2 | Inspection Rpts:P-2 Analysis | 17 |
| 3.5.1.2.2.1 | Insp. Rpts:P-2 Analysis-Reading | 17 |
| 3.5.1.2.2.2 | Insp. Rpts:P-2 Analysis-Data | 17 |
| 3.5.1.2.2.3 | Insp. Rpts:P-2 Retention | 18 |
| 3.5.1.2.3 | Inspection Rpts:P-2 User Query | 18 |
| 3.5.1.2.3.1 | Insp. Rpts:P-2 Query Type | 18 |
| 3.5.1.2.3.2 | Insp. Rpts:P-2 Query Time | 18 |
| 3.5.1.2.3.3 | Insp. Rpts:P-2 Out Of Service | 18 |
| 3.5.2 | Vehicle Data Support | 18 |
| 3.5.2.1 | Vehicle Data:Snapshots | 18 |
| 3.5.2.1.1 | Veh. Data:Snapshot Creation | 19 |
| 3.5.2.1.2 | Veh. Data:Snapshot Update | 19 |
| 3.5.2.1.3 | Veh. Data:Snapshot Retrieval | 19 |
| 3.5.3 | Driver Data Support | 19 |
| 3.5.3.1 | Driver Data:Snapshots | 19 |
| 3.5.3.1.1 | Drv. Data:Snapshot Creation. | 20 |
| 3.5.3.1.2 | Drv. Data:Snapshot Update | 20 |
| 3.5.3.1.3 | Drv. Data:Snapshot Retrieval | 20 |
| 4.0 | External Interface Requirements | 20 |
| 4.1 | Minimum User Resources | 20 |
| 4.2 | Network Connectivity Definition | 20 |
| 4.2.1 | Network Connectivity | 21 |
| 4.3 | CVIS Central Site Support | 21 |
| 4.3.1 | CVIS Census File Support | 21 |
| 4.3.1.1 | Census File Update Receipt | 21 |
| 4.3.1.2 | Census File Query | 21 |
| 4.3.1.2.1 | Census File Query Type | 21 |
| 4.3.1.2.2 | Census File Query Response | 21 |
| 4.3.1.3 | Census File Update Transmission | 22 |
| 4.3.2 | CVIS Carrier File Support | 22 |
| 4.3.2.1 | Carrier File-Full Copy | 22 |
| 4.3.2.2 | Carrier File-Updates | 22 |
| 4.3.3 | CVIS Vehicle File Support | 22 |
| 4.3.3.1 | CVIS Complete Vehicle File | 22 |

## Table of Contents


**4.3.3.2** CVIS Vehicle File Updates ..... 23
**4.3.3.2.1** Applying Vehicle File Updates ..... 23
**4.3.3.2.2** Marking Vehicle File Updates ..... 23
**4.3.4** CVIS Target File Support ..... 23
**4.3.4.1** CVIS Target File Query ..... 23
**4.3.4.1.1** Target File Query Type ..... 23
**4.3.4.1.2** Target File Query Response ..... 24
**4.3.4.2** CVIS Target File Copy ..... 24
**4.3.4.3** CVIS Target File Updates ..... 24
**4.3.4.4** CVIS MCSIP Step Update ..... 24
**4.3.4.4.1** Applying MCSIP Step Update ..... 24
**4.3.4.4.2** Logging MCSIP Step Update ..... 24
**4.3.5** CVIS Target History Support ..... 24
**4.3.5.1** CVIS Target History Creation ..... 25
**4.3.5.2** CVIS Target History Query ..... 25
**5.0** Performance Requirements ..... 25
**5.1** User Connectivity ..... 25
**5.2** Snapshot Response ..... 25
**5.3** Profile Response ..... 25
**6.0** Design Constraints ..... 25
**6.1** Privacy Considerations ..... 26
**6.2** Development Costs ..... 26
**6.3** Development Timeframes ..... 26
**6.4** Time Reference System ..... 26
**7.0** Attributes ..... 26
**7.1** Security ..... 26
**7.1.1** Data Integrity and Security ..... 26
**7.1.2** Controlled Access ..... 27
**7.1.2.1** User Access Violations ..... 27
**7.1.3** Data Access ..... **27**
**7.1.4** Privacy Requirements ..... 27
**7.1.4.1** Privacy Logging Requirements ..... 27
7.1.4.1.1 Privacy Logging Contents ..... 27
7.1.4.1.2 Privacy Logging Retention. ..... 27
**7.1.4.2** Privacy Access Requirements ..... 27
**7.1.4.2.1** Privacy Data Access ..... 28
**7.1.4.2.2** Privacy Disclosure Access ..... 28
**7.1.4.2.2.1** Privacy Disclosure Search ..... 28
**7.1.4.2.2.2** Privacy Disclosure Report ..... 28
**7.1.4.3** Privacy Data Amendment ..... 28
**7.1.4.3.1** Privacy Amendment Request ..... 28
**7.1.4.3.2** Amended Privacy Data ..... 28
**7.1.4.3.3** Amended Data Forwarding ..... 29

## Table of Contents


| | | |
|---|---|---|
| 7.1.4.4 | Privacy Agency Requirements | 29 |
| **7.2** | "ility" Requirements | 29 |
| **7.2.1** | Maintainability | 29 |
| **7.2.1.1** | Modularity | 29 |
| **7.2.1.2** | Configuration Control | 30 |
| **7.2.2** | Reusability | 30 |
| **7.2.2.1** | EDI Translation | 30 |
| **7.2.2.2** | EDI Acknowledgement | 30 |
| **7.2.3** | Reliability.. | 30 |
| **7.2.3.1** | Software Validation | 30 |
| **7.2.3.2** | System Backup | 30 |
| **7.2.4** | Availability | 31 |
| **7.3** | Data Currency | 31 |
| **8.0** | Other Requirements | 31 |
| **8.1** | Error Detection | 31 |
| **8.2** | System Management | 31 |
| **8.2.1** | Automated Logs | 31 |

# 1.0 Introduction

## 1.1 Purpose 1996

The Federal Highway Administration (FHWA) is currently testing and evaluating Intelligent Transportation Systems (ITS) technologies to enhance the safety and efficiency of interstate and intrastate commercial vehicle operations. The current focus is on creating transparent borders for interstate commercial vehicles and improving the safety of commercial vehicle operations (CVO). In support of this effort, there exists a requirement for a national CVO system that can perform numerous user services, including Automated Roadside Safety Inspections, Roadside Clearance, Onboard Safety Monitoring, Incident Management, and the Credential and Tax Administrative Process.

The Safety and Fitness Electronic Records (SAFER) System is planned as a component of ITS. One of its primary functions is to increase the efficiency and effectiveness of the inspection process at the roadside. The SAFER System will provide carrier safety historical information to fixed and mobile roadside inspection stations. This will allow roadside inspectors and other potential government and private users to focus their efforts on high-risk areas, i.e. selecting vehicles and/or drivers for inspection based on the number of prior carrier inspections and its safety history. As a result, inspection resources would be directed at drivers and vehicles associated with carriers with few prior inspections or poor safety records, while minimizing time spent inspecting carriers with many prior inspections and good safety histories. This will improve the overall cost effectiveness of the inspection process as well as provide an incentive to safe carriers.

There are many other potential functions which the System can perform. For example. SAFER will be used to support the Commercial Vehicle Information System (CVIS) which is currently conducting a feasibility study to determine if vehicle registration can be linked to carrier safety. SAFER will also provide electronic access to carrier safety information could be provided to various third party users such as shippers, insurers, vehicle rental/leasing companies and carriers themselves.

## 1.2 Scope

The SAFER System shall support US, Canadian, and Mexican interstate and intrastate carriers. SAFER will use other systems as a primary source of data, e.g. Safetynet and the Motor Carrier Management Information System (MCMIS). SAFER will provide users with electronic access to safety data via standard Electronic Data Interchange (EDI) transactions relying on other projects/entities to develop custom user interfaces to construct the requests, and display/process the responses. Data will be replicated in SAFER data bases only when required to meet performance objectives. It is envisioned that SAFER will become the mechanism for all users to acquire information about a carrier's safety fitness.

# 2.0 General Description

## 2.1 System Perspective 1996

Since the SAFER System must support short term objectives and long term goals, it will be implemented in more than one "build". Short term objectives refer to those high priority capabilities that must be deployed and will be operational by the middle of 1997, primarily providing carrier historical safety data to roadside inspection sites. However, the system architecture must also accommodate the full set of related long term ITS CVO user services/requirements, including providing, as appropriate, carrier, vehicle and driver specific safety information to state, federal, and private agencies. Development of the SAFER system must be performed in a manner consistent with the overall ITS CVO Information Systems Architecture.

## 2.2 System Functions 1996

The primary function of the System is to provide users electronic access to safety data in a timely manner via a national wide area network. This information will include identity and description of the carrier type and size, summaries of its past safety performance (inspections, accidents, other data) and its safety fitness rating.

SAFER will provide users with either a summary of a carrier's safety record ("snapshot"), or a more detailed report ("profile"). The System will be both reactive (i.e., responding to specific requests) and pro-active (i.e., allowing users to request that they be informed when the snapshot or profile changes substantially). Users will be able to request information for specific carriers or for carriers meeting certain selection criteria.

To utilize these system functions, authorized users will require, at a minimum, a computer system, a user account, and the ability to connect to the wide area network to make inquiries and receive responses. Users may wish to develop specific reporting applications tailored to their individual needs. All users, however, will receive the same basic 'packet' of information in response to a query, i.e. a transaction containing snapshot or profile information.

Other required system functions include maintenance and utility activities. SAFER must be able to ensure data currency, provide backup and security protection, and where appropriate, bill users for data exchange services.

# 3.0 Functional Requirements

## 3.1 User Services

### 3.1.1 Search/Verify a Carrier

Overview:

The System shall provide a mechanism for users to determine or verify the unique carrier identifier when it is unknown or in question. This will be accomplished through the use of a carrier matching algorithm employing fuzzy logic techniques.

In the first SAFER build, the USDOT number will provide the basis for unique carrier identification. To meet long-term SAFER requirements, the carrier ID concept must be expanded according to the following form:

Carrier ID = 'CC NNNNNNN 'TT' where,

CC = A code for issuing authority, e.g., states, provinces, etc. (to be implemented)

NNNNNNN = A sequential number, like the USDOT number or a derivative.

TT = A sub-code for a carrier denoting, for example, a specific terminal to which a vehicle is assigned. (Not yet Implemented)

Carrier Search Definition:

The input required for carrier identification is the USDOT number. If the USDOT number is not known, the System shall provide a 'searching' algorithm using, for example, ICC Number, carrier name, address, etc. as search input. If missing or erroneous data is supplied, the System shall provide users with an optional 'fuzzy' matching search algorithm.

The fuzzy searching algorithm will 'score' each candidate according to the probability of achieving an exact match. A score at or above some defined threshold will be interpreted as an exact match. Candidates with a computed score falling in between an exact match and an obvious non-match case, will be included in the supplied list.

The output of the fuzzy search process will be a scored list of potential candidates with their corresponding USDOT number.

### 3.1.1.1 Search Input

The System shall accept as input for carrier search either a unique carrier ID, or supplementary fields such as carrier name, ICC number, etc.

#### 3.1.1.1.1 Pre-Formatted Queries (M) 1996

The system shall maintain a list of standard 'pre-formatted' carrier queries. The user can issue data requests by selecting queries from the list,.

#### 3.1.1.1.2 Cost Check (M) 1997

The system shall optionally provide users with an approximate cost estimate of a data request.

### 3.1.1.2 Search Processing (M) 1996

The System shall retrieve either an exact match given a carrier ID (USDOT number), or employ a searching algorithm for retrieving a carrier ID using the supplementary data provided by a user.

#### 3.1.1.2.1 Fuzzy Searching (M) 1996

The system shall provide the option of specifying whether or not 'fuzzy' searching should be employed.

### 3.1.1.3 Search Output

In response to a query, the System shall return one of the following:

- An exact match
- A list of potential candidates determined via fuzzy matching
- A message indicating that no candidates were found

#### 3.1.1.3.1 Maximum Carriers Returned (M) 1997

When 'fuzzy' searching is employed, the system shall provide the user with an option to specify the maximum number of 'most-likely' carriers to be returned.

### 3.1.1.3.2 Multiple Match Format (M) 1996

When a query legitimately results in more than one carrier match (non-unique), the system shall provide the user with the option to specify whether the full snapshot, or census data only should be returned.

### 3.1.2 Provide Carrier Snapshot Report 1996

Overview:

A snapshot report is one which provides high-level information pertaining to: who the carrier is, where the carrier is based, and the carrier's safety rating and safety record. SAFER shall provide this information via a standard ED1 transaction which each user will process and format depending upon individual requirements. Users of snapshot data will include: electronic clearance officials, enforcement officers, shippers, insurers, leasers, and carriers.

### 3.1.2.1 Snapshot Input Definition 1996

The basic user input required for this request is the unique Carrier ID (USDOT number). If the USDOT number is unknown, the System shall employ a 'searching' algorithm to resolve input ambiguity. Snapshot data retrieved from authoritative source systems will consist of summary information from accident and inspection reports, and compliance reviews.

### 3.1.2.1.1 User Input For Snapshots (M) 1996

The System shall accept a unique Carrier ID (USDOT number) for each snapshot to be generated.

### 3.1.2.1.2 Snapshot Data Sources (M) 1996

The data required to generate the carrier snapshot shall be provided by external authoritative source systems.

### 3.1.2.1.3 Auth. Source Updates-Snapshots (M) 1996

Authoritative source systems shall supply SAFER with updated snapshot data whenever carrier safety data changes substantially.

#### 3.1.2.1.4 Snapshot Update Format (M) 1997

The system shall accept updated snapshot information from authoritative sources. The information may take the form of the census data, safety data, or both.

### 3.1.2.2 Snapshot Processing Definition

Using the unique carrier ID (USDOT number), carrier snapshot information will be retrieved, and directed to the user. Based on the request priority, the requested data may be queued for immediate transmission, or held for subsequent low priority transmission.

#### 3.1.2.2.1 Snapshot Data Extraction (M) 1996

For a requested carrier, the System shall extract the required snapshot data from a local snapshot data base.

#### 3.1.2.2.2 Snapshot Routing (M) 1996

Based on the request priority, the System shall queue the requested snapshot data for immediate transmission or hold it for subsequent low priority transmission.

#### 3.1.2.2.3 Snaps hot Refresh (M) 1996

The system shall provide a mechanism for SAFER to issue snapshot refresh requests to an authoritative source.

### 3.1.2.3 Snapshot Output Definition

The snapshot output shall consist of carrier identification, and a safety summary. A draft description of the field content of a sample snapshot report is included as an attachment to this document.

#### 3.1.2.3.1 Standard Snapshot Output (M) 1996

The System shall provide snapshot data transmitted via an accepted ED1 standard.

### 3.1.2.3.2 Snapshot Views (M) 1996

The System shall be able to provide a partial set of snapshot data, (referred to as a view), transmitted via an accepted ED1 standard. These views will be designed so that their content is tuned to the particular needs of a certain type of SAFER user. New views may be added as required, with no effect on any existing views.

## 3.1.3 Detailed Carrier Profile Report

Overview:

A profile report is one which provides detail-level information pertaining to: who the carrier is, where the carrier is based, the carrier's safety rating and safety record, and inspections and compliance reviews. SAFER shall provide this information via a standard ED1 transaction which each user will process and format according to their individual requirements. Users of profile data will include: enforcement officers, compliance reviewers, shippers, insurers, and leasers.

### 3.1.3.1 Profile Input Definition

The basic user input required for this data request is the unique Carrier ID (USDOT number). If the USDOT number is unknown, the System shall employ the 'searching' algorithm to resolve input ambiguity. Profile data retrieved from the authoritative source systems will consist of both event and summary information from accident and inspection reports, and compliance reviews.

### 3.1.3.1.1 User Input For Profiles (M) 1996

The System shall accept a unique Carrier ID (USDOT number) for each profile to be generated.

### 3.1.3.1.2 Auth. Source Input For Profiles (M) 1996

The data required to generate the carrier profile shall be provided by external authoritative source systems.

### 3.1.3.2 Profile Processing Definition 1996

Using the unique carrier ID (USDOT number). carrier profile information will be retrieved from either a temporary cache of previously requested profiles or an authoritative source, and directed to the user. Based on the request priority, the report may be queued for immediate transmission or

held for subsequent low priority transmission.

#### 3.1.3.2.1 Profile Data Extraction (M) 1996

For a requested carrier, the System shall extract the required profile data from the appropriate source, i.e. external authoritative source system or locally held copy.

#### 3.1.3.2.2 Profile Routing (M) 1996

Based on the request priority, the System shall queue the requested profile data for immediate transmission or hold it for subsequent low priority transmission.

#### 3.1.3.2.3 Duplicate Profile Requests (M) 1996

The system shall be capable of recognizing duplicate profile requests from the same user. It will ignore duplicate requests and inform the user of its action.

#### 3.1.3.2.4 Pending Profile Data (M) 1996

The system shall maintain a list of external profile requests pending data receipt from an authoritative source. Use of this list, will ensure that redundant requests for the same carrier profile will not be sent to an authoritative source.

### 3.1.3.4 Profile Outputs Definition

Profile output shall consist of a series of records describing a variety of safety-related aspects of carrier operations. A draft description of the field content of a sample profile report is included as an attachment to this document.

#### 3.1.3.4.1 Standard Profile Output (M) 1996

The System shall provide profile data transmitted via an accepted EDI standard.

#### 3.1.3.4.2 Profile Cache (M) 1996

Within time/storage constraints, the system shall maintain a cache of recently-received

carrier profiles. This will allow more than one user request for the same carrier to be serviced from a single request to an authoritative source. After a period of time (TBD) the profiles will be deleted.

### 3.1.4 Carrier "Subscriber" Capability 1996

Overview:

The Subscriber list capability allows a user to monitor a group of user-specified carriers. To support this concept, SAFER shall provide a Subscriber list facility whose requisite parts are:

- A user-defined list of carriers to monitor.
- A user-defined response priority, i.e. immediate or queued.
- A user-defined list of conditions or thresholds used to trigger a Subscriber list response.

Subscriber list users will include: enforcement officers, shippers, insurers, leasers, and carriers. The Subscriber list response shall consist of snapshot data for carriers who have exceeded a Subscriber list threshold.

Subscriber **List Input Definition:**

Required user input for Subscriber list processing consists of a list/group of carrier **USDOT** numbers and a set of conditions, or thresholds which trigger a Subscriber response. A set of Subscriber list thresholds will be provided to the user to facilitate the Subscriber list definition process. Example threshold conditions are provided below:

- A carrier's CVIS Safestat score changes from one range of values to another,
- A carrier's safety rating changes,
- A carrier's compliance review information changes.

#### 3.1.4.1 Subscriber List Input (M) 1996

The System shall accept user input consisting of carriers of interest (USDOT Numbers, or other selection criteria), and threshold values as the basis for defining a Subscriber list.

#### 3.1.4.2 Subscriber List Processing

Subscriber list Processing Definition:

Subscriber list processing will be performed by the SAFER system. Authoritative source systems will pro-actively notify SAFER whenever certain types of safety data change (an event) for

any carrier. SAFER, in turn, will notify the appropriate users via transmittal of updated carrier snapshots or profiles.

#### 3.1.4.2.1 Subscriber List Trigger Process (M) 1996

The System shall trigger a Subscriber list response whenever an event threshold value is met or exceeded.

#### 3.1.4.2.2 Threshold/Event Translation (M) 1996

The System shall translate user defined thresholds into corresponding events monitored by authoritative source systems.

#### 3.1.4.2.3 Update Event Table (M) 1996

The System shall provide a method of updating the current set of carrier events being monitored. The system shall be capable of electronically transmitting this updated information to users and authoritative sources. Each update to the event table shall be uniquely defined by an 'Event Update Date'.

#### 3.1.4.2.4 Automated Subscriber Update (M) 1997

When updating the current set of carrier events being monitored, the System shall be capable of automatically updating existing subscriber lists to ensure consistency with the newly defined list of events. The System shall automatically notify users of any changes to the event list.

#### 3.1.4.2.5 Types of Events Monitored (M) 1996

The System shall monitor two types of events. A 'simple change' to a field, and a 'range change' to a field which causes it to move from one level of predefined value ranges to another.

#### 3.1.4.2.6 Determination of Event (M) 1996

Upon receipt of updated snapshot information from an authoritative source, the system shall be capable of determining which event triggered the generation of each snapshot. This information will not be provided by authoritative sources.

### 3.1.4.2.7 Subscriber Response Time (M) 1996

The System shall allow a Subscriber to specify whether he should be sent responses to his criteria pro-actively (as they occur), or periodically (batched and sent weekly, monthly, etc.).

### 3.1.4.3 Subscriber List Output Def.

Subscriber list output shall consist of snapshot/profile data provided to the user whenever an event threshold has been met or exceeded.

### 3.1.4.3.1 Subscriber List Output (M) 1996

Whenever a Subscriber list threshold has been met or exceeded, the System shall provide users with the appropriate snapshot/profile data via a user-specified immediate or low priority transmission.

### 3.1.4.3.2 Event Monitoring Report (M) 1996

The system shall be capable of generating a report describing the current set of carrier events being monitored.

### 3.1.4.3.3 Subscriber Status Report (M) 1996

The system shall provide a method which allows a user to examine his current subscriber list.

### 3.1.4.4 Subscriber User Update (M) 1996

The System shall allow the user to designate whether the object of a query (carrier, vehicle, or driver) shall be included in the user's subscription list so that all future subscription-related updates shall consider the designated entity. In this case, if the user has more than one subscription list, the System shall allow the user to designate to which subscription the entity shall be added.

### 3.1.5 Aggregate Data Requests 1996

Overview:

Users may wish to store snapshot data for groups of carriers (e.g., all carriers domiciled in a particular state) within a locally defined information system. To facilitate this capability, the System shall provide a mechanism for creating groups of carrier snapshots for delivery to the user

via external files or on-line transmission.

### 3.1.5.1 Aggregate Data Request Input (M) 1996

The System shall accept as input a list of carriers or other criteria, such as geographic location, to be used to select snapshot data to be provided to the user.

### 3.1.5.2 Aggregate Data Req. Processing (M) 1996

The System shall optionally provide requesting users a complete set of snapshot data corresponding to a subscriber list definition.

### 3.1.5.3 Aggregate Data Request Output (M) 1996

The System shall provide snapshot data to external users via an external file or an on-line transmission.

## 3.2 Establish/Maintain User Account

Overview:

Each authorized user (whether internal or external) will establish a valid account to access the SAFER system.

### 3.2.1 User Account Input (M) 1996

To establish an account, the System shall require that users provide the System with certain forms of identification information such as name, address, etc.

### 3.2.1.1 Organizational Account (M) 1996

The system shall be capable of establishing user accounts on behalf of an organization. An organization my have one or more valid users.

### 3.2.2 User Account Processing 1996

The system shall be capable of registering new users, maintaining user accounts, and providing account update and view capabilities.

### 3.2.2.1 User Account Update Processing (M) 1996

The System shall provide users with the capability of updating certain user account information.

### 3.2.2.2 User Account Access Privilege (M) 1996

The System shall provide the capability of restricting access to data having privacy implications.

### 3.2.2.3 Request Cancellation (M) 1997

The system shall allow a user to cancel certain types of data requests.

### 3.2.2.4 User Requests Waiting (M) 1996

The system shall maintain a list of all data requests waiting to be sent to a user, thereby facilitating low/overnight priority processing.

### 3.2.3 User Account Output 1996

The system shall make available an account summary for each user, specifying access privileges, etc.

### 3.2.3.1 User Account Status Fields (M) 1996

The System shall establish and maintain a user account which will be made available to the user for read only access.

### 3.2.3.2 User Documentation (M) 1996

Users shall be provided a set of System documentation in either hardcopy or electronic form.

### 3.2.3.3 User Software (M) 1996

Users shall be provided with generic interface software developed during system test and evaluation.

## 3.3 Monitor System Activity/Billing 1996

Definition:

The System shall monitor all user activity. For certain users, charges will be computed for selected system services. System activity reports will be generated and utilized in management and billing operations, and as a means of judging effectiveness of operations. Example entries in a syste activity report are presented below:

- Number of log-ins and average session time (by userid and total)
- Number of responses generated, and lines/bytes transmitted (by userid and total)
- SAFER communication links to authoritative source data systems (number of connections, average connect time, and volume of data transmitted)
- Accounts receivable (by userid, for the current billing period and year)
- Individual account bills which may be mailed/transmitted to the appropriate user

### 3.3.1 System Activity Logging (M) 1996

The System shall log all user activity and provide a mechanism for generating reports for management and billing operations.

### 3.3.2 Privacy Access Transaction Log (M) 1996

If SAFER is determined to be a Federal system, a transaction log itemizing each request for information about a specific driver shall be created and maintained for six years. Further details may be found under 'Privacy Requirements'.

### 3.3.3 Network Billing (D) 1997

The system shall be capable of generating an automated billing report (if available) describing network usage costs.

## 3.4 External System Data Access 1996

Definition:

The System will serve as an electronic data interchange for safety data residing in authoritative source systems. The first data interfaces to be implemented will be with MCMIS and the inspection sites associated with the 200 MCSAP Site Project. An interface to Safetynet will be implemented in the next System build.

### 3.4.1 Accessing Authoritative Sources (M) 1996

The System shall include an electronic interface to MCMIS to retrieve safety related data.

### 3.4.1.1 Authoritative Source Ack. (M) 1996

The system shall ensure that an acknowledgment is received for each data request. If an acknowledgment is not received in a specified period of time (TBD), the system shall take appropriate action (issue error message, re-send request, etc).

### 3.4.1.2 Authoritative Src. Data Receipt (M) 1996

The system shall ensure that the requested data from an authoritative source is received. If the data is not received in a specified period of time (TBD), the system will take appropriate action (issue error message, non-response log, etc).

### 3.4.2 Access Roadside Inspection Site (M) 1996

The System shall include an electronic interface to the inspection sites associated with the 200 MCSAP Site Project to retrieve and send safety related data.

### 3.4.3 Inter-User Data Flow Definition

The SAFER system shall allow users to exchange data. This feature will enable inspection data to be transferred from inspection sites to the Safetynet site in the carrier's state of domicile.

### 3.4.3.1 Inter-User Data Exchange (M) 1997

The System shall provide a mechanism for users to exchange safety data.

### 3.4.3.2 Inter-User Data Routing (M) 1997

The System shall automatically provide network routing information to inter-user data exchanges.

### 3.4.4 Base State Routing (M) 1996

The system shall maintain a base-state routing table. This table will link a carrier's state of domicile, the corresponding authoritative source, and certain system information (network address, etc.)

## 3.5 Vehicle/Driver Data Support (M)

The System shall provide a mechanism for support of data relating to Commercial Vehicles and Drivers. The initial method of acquisition of this the of data will be via the electronic receipt of Inspection reports. Requirements specified below are grouped under the general headings of: Inspection Reports, Vehicle, and Driver. The requirements are also distinguished as either Phase1 or Phase2, indicating two incremental levels of capability to be implemented in succession.

### 3.5.1 Inspection Report Support (M)

The System shall provide a mechanism for electronically receiving, storing, and distributing inspection reports. The inspection reports are initially created at the roadside by safety enforcement officers. SAFER system inspection-handling capabilities will be implemented in the two progressive phases which are described below.

### 3.5.1.1 Inspection Reports:Phase 1 (M) 1996

The System shall (in Phasel) provide a mechanism for electronically receiving, temporarily storing, and allowing access to inspection reports. All of these activities will be conducted via the **SAFER** Data Mailbox environment.

### 3.5.1.1.1 Inspection Rpts:P-1 Receipt (M) 1996

The System shall (in Phasel) provide a mechanism for users to electronically send standardized inspection reports to the SAFER Data Mailbox. The transmission format will be a text file, possibly employing some compaction techniques. Users may send reports at their convenience (a 'transmission session' with SAFER will not have to be scheduled).

### 3.5.1.1.2 Inspection Rpts:P-1 Storage (M) 1996

The **System shall (in Phasel) provide** a mechanism for electronically storing inspection reports via the SAFER Data Mailbox for later access by the appropriate Safetynet Site. The inspection reports will be stored in the same format 'as originally received'.

### 3.5.1.1.3 Inspection Rpts:P-1 Deletion (M) 1996

The System shall (in Phasel) determine when the a Safetynet Site has retrieved an inspection report. Once the retrieval is completed, the report will be deleted from the SAFER Data Mailbox.

### 3.5.1.1.4 Insp. Rpts:P-1 Mailbox Access (M) 1996

The System shall (in Phasel) provide a mechanism with which users may access inspection reports using mailbox techniques. Users may access reports at their convenience (a 'transmission session' from SAFER will not have to be scheduled).

### 3.5.1.2 Inspection Reports:Phase 2 (M) 1996

The System shall (in Phase 2) continue to provide a mechanism for electronically receiving, temporarily storing, and allowing access to inspection reports. The 'electronic mailbox' environment **for receiving and sending will continue to be supported. In addition, fI eld-level data from within the** report will now also be extracted and stored elsewhere. Some User query activity will be supported.

### 3.5.1.2.1 Insp. Rpts:P-2 Mailbox Access (M) 1996

The System shall (in Phase2) continue to provide a mechanism with which users may access specific inspection reports using mailbox techniques. Specific access requirements are identical to those found under 'Inspection Reports:Phase- **1'.**

### 3.5.1.2.2 Inspection Rpts:P-2 Analysis (M) 1996

The System shall (in Phase2) perform a simple analysis of incoming inspection reports in order to determine the general nature of the report. In addition, the individual report fields will be extracted and saved into tables for subsequent use. See also-Vehicle Data Support' and 'Driver Data support'

### 3.5.1.2.2.1 Insp. Rpts:P-2 Analysis-Reading (M) 1996

The System shall (in Phase2) be able to identify an incoming transaction as an inspection report, and apply appropriate compaction techniques (eg. 'unzipping') in order to read information from the report.

### 3.5.1.2.2.2 Insp. Rpts:P-2 Analysis-Data (M) 1996

The System shall (in Phase2) be able to extract from an incoming inspection report, all of the data fields contained within a report and store these fields into tables for subsequent use.

### 3.5.1.2.2.3 Insp. Rpts:P-2 Retention (M) 1996

The System shall (in Phase2) extract the date and time of the inspection and use that information to retain (on the System) each inspection report for thirty days.

### 3.5.1.2.3 Inspection Rpts:P-2 User Query (M) 1996

The System shall (in Phase2) provide a mechanism with which users may query the system for specific inspection reports and obtain report copies.

### 3.5.1.2.3.1 Insp. Rpts:P-2 Query Type (M) 1996

The System shall (in Phase2) support several types of user queries for inspection reports. The query fields are: l-Inspection Report Number, 2-Vehicle License Plate/State, 3-Driver ID Number (See 'Privacy Requirements' for requirements related to driver).

### 3.5.1.2.3.2 Insp. Rpts:P-2 Query Time (M) 1996

The System shall (in Phase2) support the following types of time-related options pertaining to user queries for inspection reports. The options are: l-Return the most recent Inspection Report. 2--Return all of the Inspection Reports on hand within the thirty-day retention period.

### 3.5.1.2.3.3 Insp. Rpts:P-2 Out Of Service (M) 1996

The System shall (in Phase2) support the following types of out of service options pertaining to user queries for inspection reports. The options are: l-Return the most recent Inspection Report which resulted in an out of service condition. 2--Return all of the Inspection Reports on hand within the thirty-day retention period which resulted in an out of service condition.

### 3.5.2 Vehicle Data Support (M) 1996

The System shall provide a mechanism for support of data relating to Commercial Vehicles. The initial method of acquisition of this data will be via the electronic receipt of Inspection reports. Requirements specified below refer to implementation Phases (see 'Inspection Reports Support' for more information concerning the Phases).

### 3.5.2.1 Vehicle Data:Snapshots (M) 1996

The System shall (in Phase2) provide a mechanism which allows creation, storage and retrieval of vehicle snapshots.

### 3.5.2.1.1 Veh. Data:Snapshot Creation (M) 1996

The System shall (in Phase2) provide a mechanism which will add a new entry to the vehicle snapshot database. As inspection reports are recieved, if no Snapshot is currently held for the Vehicle in question, a new snapshot is created. The new snapshot is populated only with appropriate data available within the inspection report, and some fields within the snapshot definition may be temporarily left blank

### 3.5.2.1.2 Veh. Data:Snapshot Update (M) 1996

The System shall (in Phase2) provide a mechanism which will update an entry in the vehicle snapshot database. As inspection reports are recieved, if a Snapshot is currently held for the Vehicle in question, the existing snapshot is updated. The fields to be updated are those which might have changed (for example, the date of last inspection). The 'date of last update' is changed appropriately.

### 3.5.2.1.3 Veh. Data:Snapshot Retrieval (M) 1996

The System shall (in Phase2) provide a mechanism which will allow a user to query for a specific vehicle snapshot. The query criteria initiallly supported will be via the License plate number, and state, or Vin number. If no Snapshot is currently held for the Vehicle in question, the system will return an appropriate message (Eg., 'Sorry, no data available').

### 3.5.3 Driver Data Support (M) 1996

The System shall provide a mechanism for support of data relating to Drivers of Commercial Vehicles. Privacy considerations in relation to driver identity are specified in 'Privacy Requirements' and apply to all the requirements found below. The initial method of acquisition of this data will be via the electronic receipt of Inspection reports. Requirements specified below refer to

implementation Phases (see 'Inspection **Reports** Support' for more information concerning the Phases)

### 3.5.3.1 Driver Data:Snapshots (M) 1996

The System shall (in Phase2) provide a mechanism which will support creation, storage and retrieval of driver snapshots.

### 3.5.3.1.1 Drv. Data:Snapshot Creation (M) 1996

The System shall (in Phase2) provide a mechanism which will add a new entry to the driver snapshot database. As inspection reports are recieved, if no Snapshot is currently held for the driver in question, a new snapshot is created. The new snapshot is populated only with appropriate data available within the inspection report, and some fields within the snapshot definition may be temporarily left blank

### 3.5.3.1.2 Drv. Data:Snapshot Update (M) 1996

The System shall (in Phase2) provide a mechanism which will update an entry in the driver snapshot database. As inspection reports are recieved, if a Snapshot is currently held for the driver in question, the existing snapshot is updated. The fields to be updated are those which might have changed (for example, the date of last inspection of that driver). The 'date of last update' is changed appropriately.

### 3.5.3.1.3 Drv. Data:Snapshot Retrieval (M) 1996

The System shall (in Phase2) provide a mechanism which will allow a user to query for a specific driver snapshot. All such queries are subject to the restrictions specified under 'Privacy Requirements', in Section 7.1.4 . The query criteria initially supported will be via the Driver ID number. If no Snapshot is currently held for the Driver in question, the system will return an appropriate message (Eg., 'Sorry, no data available').

## 4.0 External Interface Requirements

### 4.1 Minimum User Resources (M) 1996

Users shall be capable of accessing the SAFER system with the following minimum hardware and

software configuration:

- A completed, approved application for a user account
- A computer system
- The ability to connect to the wide area network
- Interface Software

## 4.2 Network Connectivity Definition

SAFER system electronic data interchange operations shall be performed via a national wide area network. Users will access the System using standard communications software.

### 4.2.1 Network Connectivity (M) 1996

The System shall make use of a wide area network to effect electronic data exchange.

## 4.3 CVIS Central Site Support (M) 1996

The System shall provide Central Site support of the Commercial Vehicle Information System (CVIS) and the associated Motor Carrier Safety Improvement Program (MCSIP). Requirements specified below are grouped to describe the appropriate CVIS concept, but stated in terms of the SAFER environment.

### 4.3.1 CVIS Census File Support (M) 1997

The System shall provide maintenance, update, and query support of the CVIS Census File. The Census file is logically equivalent to the set of carriers within the SAFER Carrier Snapshot database. The requirements specified below will be supported from within the SAFER Carrier Snapshot database.

#### 4.3.1.1 Census File Update Receipt (M) 1997

The System shall, on a daily basis, receive updated Carrier information from MCMIS and apply the updates to the SAFER Carrier Snapshot database.

#### 4.3.1.2 Census File Query (M) 1997

The System shall allow CVIS users to interactively query the SAFER Carrier Snapshot database via an X12 type 285 ED1 transaction.

#### 4.3.1.2.1 Census File Query Type (M) 1997

The System shall, provide to CVIS users, query capability into the SAFER Carrier Snapshot database based on either USDOT Number or Motor Carrier Name.

#### 4.3.1.2.2 Census File Query Response (M) 1997

The System shall, provide in response to a query, a SAFER Carrier Snapshot either in complete form, or if requested, a specific snapshot view.

#### 4.3.1.3 Census File Update Transmission (M) 1997

The System shall, on a daily basis, transmit (to appropriate CVIS users) the SAFER Carrier Snapshot updates received for that day. The transmission shall be via file format.

### 4.3.2 CVIS Carrier File Support (M) 1997

The System shall provide maintenance, update, and query support of the CVIS Carrier File. The carrier file is logically equivalent to those carriers within the SAFER Carrier Snapshot database which are currently in the MCSIP Program. The requirements specified below will be supported from within the SAFER Carrier Snapshot database.

#### 4.3.2.1 Carrier File-Full Copy (M) 1997

The System shall provide on request, a complete copy of the CVIS Carrier File. This carrier file copy will consist of all of the carriers within the SAFER Carrier Snapshot database which are currently in the MCSIP Program.

#### 4.3.2.2 Carrier File-Updates (M) 1997

The System shall provide to CVIS users, the daily updates to the CVIS Carrier File, This carrier file update will consist of the carriers within the SAFER Carrier Snapshot database which are currently in the MCSIP Program, and for whom an updated snapshot was received that day.

### 4.3.3 CVIS Vehicle File Support (M) 1997

The System shall accept updates to, and provide maintainence for the CVIS Vehicle File. The vehicle file is logically equivalent to the set of vehicles registered to carriers within the SAFER Carrier Snapshot database which are currently in the MCSIP Program. The requirements specified below will be supported from within the SAFER Vehicle Snapshot database.

### 4.3.3.1 CVIS Complete Vehicle File (M) 1997

The System shall on request, accept a full CVIS Vehicle File from a CVIS state. The vehicle file is to be applied to the SAFER Vehicle Snapshot database in time for the next day's business.

### 4.3.3.2 CVIS Vehicle File Updates (M) 1997

The System shall receive and process updates to the CVIS Vehicle File throughout the business day. The updates will be sent by CVIS states on an 'as necessary' basis via an Xl2 type 285 ED1 transaction.

### 4.3.3.2.1 Applying Vehicle File Updates (M) 1997

The System shall apply updates to the CVIS Vehicle File as they are received throughout the business day. Application of the update will take the form of either updating an existing snapshot in the SAFER Vehicle Snapshot database or creating a new one.

### 4.3.3.2.2 Marking Vehicle File Updates (M) 1997

The System shall mark updates to the CVIS Vehicle File as they are applied throughout the business day via the 'Date of Last Update' field. This action is required in order to support CVIS users who maintain a CVIS Target file locally. See also 'CVIS Target File Support'.

### 4.3.4 CVIS Target File Support (M) 1997

The System shall maintain, provide updates, and provide query capability for the CVIS Target File. The Target file is logically equivalent to the set carriers within the SAFER Carrier Snapshot database which are currently in the MCSIP Program, and the vehicle snapshots which represent the vehicles registered to those carriers. The requirements specified below will be supported from within the SAFER Carrier and Vehicle Snapshot databases.

### 4.3.4.1 CVIS Target File Query (M) 1997

The System shall provide an interactive query capability (via an Xl2 type 285 ED1 transaction) for the CVIS Target File. The queries and responses will be supported from within the SAFER Carrier and Vehicle Snapshot databases.

### 4.3.4.1.1 Target File Query Type (M) 1997

The System shall provide query capability (via an Xl2 type 285 ED1 transaction) for the CVIS Target File based on the following criteria: The user may specify Carrier via USDOT Number, or vehicle via either vehicle license-plate and state, or Vehicle Identification Number (VIN).

### 4.3.4.1.2 Target File Query Response (M) 1997

In response to an interactive query to the CVIS Target File, the System shall provide Carrier and/or Vehicle Snapshots (per user option). At the user's request, the snapshots could take either a complete form, or a more compact 'view'.

### 4.3.4.2 CVIS Target File Copy (M) 1997

The System shall provide on request, a complete copy of the CVIS Target File. The transmission will be done via file transfer, and will logically consist of the Carrier and associated Vehicle Snapshots for all those carriers currently in the MCSIP program.

### 4.3.4.3 CVIS Target File Updates (M) 1997

The System shall provide (to appropriate users) updates to the CVIS Target File as transactions are received during the business day. See also 'CVIS Vehicle File Updates'.

### 4.3.4.4 CVIS MCSIP Step Update (M) 1997

The System shall provide a mechanism to allow an authorized CVIS user to update the 'MCSIP Step' in the SAFER Carrier Snapshot corresponding to a carrier currently in the MCSIP program.

### 4.3.4.4.1 Applying MCSIP Step Update (M) 1997

After receipt of a properly authorized request, the System shall provide a mechanism which

will allow the 'MCSIP Step' field within a carrier snapshot to be updated in the SAFER database.

#### 4.3.4.4.2 Logging MCSIP Step Update (M) 1997

Before the MCSIP Step of a carrier may be updated, the System shall log the activity by (at a minimum), creating an entry in the CVIS Target History File. See also 'CVIS Target History File'.

### 4.3.5 CVIS Target History Support (M) 1997

The System shall maintain and provide query capability for the CVIS Target History File. The Target History file is logically equivalent to the 'before' images of carrier and vehicle snapshots in the CVIS Target File for which updates have been processed. The requirements specified below will be supported from within tables similar to the SAFER Carrier and Vehicle Snapshot databases, but held separately.

#### 4.3.5.1 CVIS Target History Creation (M) 1997

The System shall create entries in the CVIS Target History File whenever a CVIS Target File entry is being updated. The 'before' images of carrier and/or vehicle snapshots about to be updated will be written to the Target History tables maintained within SAFER.

#### 4.3.5.2 CVIS Target History Query (M) 1997

The System shall provide query capability for the CVIS Target History File. The query types and responses shall be identical to those which are provided for the Target File. See also 'CVIS Target File Query'.

## 5.0 Performance Requirements

### 5.1 User Connectivity (M) 1996

The System shall have the capability of processing concurrent user requests. The maximum number of concurrent requests will be defined during system design.

### 5.2 Snapshot Response (M) 1996

The System shall provide either an immediate or a delayed queued response to a snapshot request. The exact response times **will** be defined during system design.

### 5.3 Profile Response (M) 1996

The System shall provide either an immediate or a delayed queued response to a profile request. The exact response times will be defined during system design.

## 6.0 Design Constraints

### 6.1 Privacy Considerations (M) 1996

The System shall ensure that all right-to-privacy laws are observed. Systematic checks shall verify that only those agencies/entities having the necessary access privileges will receive access to restricted data. Unauthorized access attempts shall be recorded in the system activity log. Specific privacy requirements are itemized under 'Privacy Requirements'.

### 6.2 Development Costs (M) 1997

The SAFER system costs shall not exceed the monetary appropriations allocated to the project.

### 6.3 Development Timeframes (M) 1997

The SAFER system development shall be completed within the timeframe necessary to satisfy the Congressional mandate for the 100/200 MCSAP Site Project.

### 6.4 Time Reference System (M) 1996

The system shall employ a single time reference system, i.e., Greenwich Mean Time. This will eliminate potential problems between users/nodes in different time zones.

## 7.0 Attributes

## 7.1 Security

Definition:

The SAFER system shall ensure the integrity of all safety data transactions. Data integrity shall be maintained through the use of access controls and encryption.

### 7.1.1 Data Integrity and Security (M) 1996

The System shall be secure from unauthorized modification of data and other system entities.

### 7.1.2 Controlled Access (M) 1996

The System shall only allow access to authorized users.

#### 7.1.2.1 User Access Violations (M) 1996

The system shall maintain a table of user access violations to support system security functions.

### 7.1.3 Data Access (M) 1996

The System shall provide the capability of restricting user access to certain safety data and user account information.

### 7.1.4 Privacy Requirements (M) 1996

The SAFER System shall comply with all applicable privacy laws.

#### 7.1.4.1 Privacy Logging Requirements (M) 1996

The SAFER System shall log disclosures made as a result of query by Driver **Name** or ID Number.

##### 7.1.4.1.1 Privacy Logging Contents (M) 1996

For Driver disclosures (except for FHWA requests), the SAFER System shall log the following items:

the date, type of request material transmitted, and name and address of the user to whom the disclosure was made.

#### 7.1.4.1.2 Privacy Logging Retention (M) 1996

For Driver disclosures, the SAFER System shall maintain the logging information for at least six years after the disclosure was made.

#### 7.1.4.2 Privacy Access Requirements (M) 1996

The SAFER System shall provide to Drivers, access to stored information and disclosures made as a result of SAFER operations.

#### 7.1.4.2.1 Privacy Data Access (M) 1996

On request, the SAFER System shall provide to Drivers, a comprehensible copy of currently-stored (within SAFER) information pertaining to him.

#### 7.1.4.2.2 Privacy Disclosure Access (M) 1996

On request, the SAFER System shall provide to Drivers, a comprehensible copy of the log of disclosures made pertaining to him as described under the 'Privacy Logging Requirement' above.

#### 7.1.4.2.2.1 Privacy Disclosure Search (M) 1996

The SAFER System shall provide a method to search the Privacy disclosure log, selecting and storing all entries associated with a specific Driver Id.

#### 7.1.4.2.2.2 Privacy Disclosure Report (M) 1996

The SAFER System shall provide a method to format a report containing the data stored during the Privacy Disclosure Search described above. The report should be generated in a form such that it may be transmitted electronically, or printed to hardcopy.

#### 7.1.4.3 Privacy Data Amendment (M) 1996

The SAFER System shall support the data ammendment process for privacy-related information and

disclosures.

#### 7.1.4.3.1 Privacy Amendment Request (M) 1996

The SAFER System shall accept a written request to ammend information pertaining to a driver. A record of this request will be made within SAFER, and the request forwarded to the appropriate authoritative source. If, over time, the volume of these types of requests becomes high, SAFER will provide an electronic form and procedure for the task.

#### 7.1.4.3.2 Amended Privacy Data (M) 1996

On the ocassion when information is changed as a result of an ammendment request, the SAFER System shall accept the ammended information from the authoritative source and update the appropriate in-house data bases.

#### 7.1.4.3.3 Amended Data Forwarding (M) 1996

On the ocassion when information is changed as a result of an ammendment request, the SAFER System shall forward the ammended information to those persons or agencies previously sent information as described under the 'Privacy Logging Requirement' above. This only applies to data marked as 'corrected, and does not apply to data updated in normal authoritative source production operations.

### 7.1.4.4 Privacy Agency Requirements (M) 1996

Prior to establishment or revision of the system, a representative of the SAFER System shall publish in the Federal Register, a notice of the existence and character of the system of records held. Information published shall include the following:

A-The name and location of the system.
B-The categories of individuals on whom records are maintained.
C-The categories of records maintained.
D-Routine uses of the records contained in the system, including the categories of users and the purpose of such use.
E-Policies and practices regarding storage, retrievability, access controls, retention, and disposal of the records.
F-The title and business address of the agency official who is responsible for the system of records.
G-The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him
H-The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained **in** the system of records, and how he can contest its

content.
I-The categories of sources of records in the system.

## 7.2 "ility" Requirements

Definition:

The "ility" requirements describe general system requirements for availability, reliability, reusability and maintainability.

### 7.2.1 Maintainability

#### 7.2.1.1 Modularity (M) 1996

The System software shall be written using modular and structured techniques as defined in the Software Development Plan (SDP).

#### 7.2.1.2 Configuration Control (M) 1996

The System software shall be maintained using configuration control techniques as defined in the Operations and Maintenance Plan (OMP).

### 7.2.2 Reusability (M) 1996

The System shall be developed taking maximum advantage of commercially available software and re-useable code.

#### 7.2.2.1 ED1 Translation (M) 1996

The system shall employ a commercially available ED1 Translator for use in both input and output. The translator shall convert ED1 transactions from/to SAFER application format.

#### 7.2.2.2 ED1 Acknowledgement (M) 1996

The system shall provide standard ED1 acknowledgements.

### 7.2.3 Reliability

#### 7.2.3.1 Software Validation (M) 1996

The System software shall be validated by developing and using organized test procedures as defined in the Master Test Plan (MTP).

#### 7.2.3.2 System Backup (M) 1996

The System shall be protected by backup procedures.

### 7.2.4 Availability (M) 1996

The System shall be available continuously. Maintenance of the System shall be performed without significantly degrading system performance.

## 7.3 Data Currency 1996

Overview:

The SAFER system shall ensure that data, made available for electronic data interchange, is as current as possible given the rate at which data is pro-actively transmitted to SAFER from Authoritative Sources, and the data transmission criteria being satisfied by subscriber list processing.

# 8.0 Other Requirements

## 8.1 Error Detection (M) 1996

The System shall provide for the detection of and speedy recovery from errors. The System shall perform error tracing, error printing/display and termination of affected input/output processes.

## 8.2 System Management (M) 1996

The System shall have an audit trail of all system activity. The audit trail shall include, at a minimum, the following items:

Transaction type
Requestor Identifying Information
Time/Date Stamp
Transaction status (completed, incomplete, etc.)

### 8.2.1 Automated Logs (M) 1996

The system shall employ automated tools to manage/maintain various SAFER system logs (error, internal transaction, user messages).